☑ Original ☐

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
information associated with tjaquanwilson674@gmail.com that is stored at premises owned, maintained, controlled, or operated by Apple Inc. (Fully described in Attachment A)

Case No. 22-M-433 (SCD)

Matter No.: 2022R00114

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

See Attachment A. Over which this Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal Procedure 41.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 5-5-22 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Stephen C. Dries.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 4-21-22 3:00 pm

Stephen C. Dries
Judge's signature

City and state: Milwaukee, WI

Hon. Stephen C. Dries, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with jaquanwilson674@gmail.com that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B
Particular Things to be Seized

1. Information to be disclosed by Apple (Provider)

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserve, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A from 01/01/2021 to the present:

- All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses,

Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

- The contents of all emails associated with the account from 01/01/21 to present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;
- The contents of all instant messages associated with the account 01/01/21 to present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

- The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;
- All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;
- All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;
- All records pertaining to the types of service used;

- All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and
- All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

2. **Information to be seized by the government**

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C § 922 (g)(1) Felon in Possession of a Firearm and violations of 18 U.S.C. § 922(a)(6), commonly referred to as "lying and buying," those violations involving Jaquan Wilson and occurring after 01/01/21, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Records containing the sale/purchase order of ammunition in a illegal format that is intended for the military/law enforcement that would not be for public use. Records can be contained in emails, text messages, SMS messages, iMessages, etc.

(b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(e) The identity of the person(s) who communicated with the user ID about matters relating to the conspiracy and illegal importation of ammunition, including records that help reveal their whereabouts.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

information associated with tjaquanwilson674@gmail.com that is stored at premises owned, maintained, controlled, or operated by Apple Inc. (Fully described in Attachment A)

Case No. 22-M-433 (SCD)

Matter No.: 2022R00114

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A. Over which this Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal Procedure 41.

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C § 922(a)(6); 18 U.S.C. 922(g)(1)	Felon in possession of a firearm; straw purchasing.

The application is based on these facts:

See attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA Frank Rutter, ATF

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 4-21-22

Judge's signature

City and state: Milwaukee, WI

Hon. Stephen C. Dries, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Frank Rutter, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am employed with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and have been since 2015. As an ATF Agent, I have conducted numerous investigations involving violations of federal and state laws including violations of 18 U.S.C. § 922(a)(6), commonly referred to as "lying and buying" as well as investigations related to the unlawful use/possession of firearms and firearms trafficking; investigations involving violations of 21 U.S.C. § 841(a)(1) and 846 (conspiracy to possess with the intent to distribute and distributing a controlled substance). I have had a variety of formal, informal, and on the job training in the

investigation of illegal firearms possession and firearms trafficking; I have participated in the execution of search warrants in which firearms, ammunition and controlled substances were seized; and I am familiar with the street name(s) of firearms, controlled substances and respective related topics.

3. The facts in this affidavit come from my personal observations, my training and experience, and from information obtained from other investigators and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C § 922 (g)(1), Felon in Possession of a Firearm and violations of 18 U.S.C. § 922(a)(6), commonly referred to as "lying and buying" have been committed and that evidence of those violations is contained in following Apple iCloud account: jaquanwilson674@gmail.com, which is linked to the owner, Jaquan WILSON. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

3. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

4. On July 29, 2021, the Wisconsin State Patrol (WSP) conducted a traffic stop on a vehicle traveling northbound on Interstate 41 in Appleton, Wisconsin located within the Eastern District of Wisconsin. The vehicle can be described in more detail as a 2014, white in color, Toyota bearing Wisconsin license plate CB34802 and VIN: 4T1BD1FK7EU103830. The driver and sole occupant, identified as Jaquan M. Wilson (DOB: 1994), was arrested for several offenses including felon in possession of a firearm. Recovered from the vehicle were numerous items of evidentiary value including, but not limited to, two (2) firearms, suspected marijuana, a Dremel set and a black Apple iPhone with a Kobe Bryant case. Affiant is aware that one (1) of the recovered firearms had an obliterated serial number. The firearms can be described in further detail as:

- Manufacturer: Sarsilmaz, Importer: SAR USA, Model: SAR 9, Caliber: 9mm, SN: T1102-21BV87638, Type: Pistol; and
- Manufacturer: Taurus, Importer: Taurus International, Model: The Judge, Caliber: 45/410, SN: OBLITERATED, Type: Revolver.

5. Wilson has a felony conviction from Cook County, Illinois, Case 2013CR155110 for Armed Robbery, and he is therefore Federally prohibited from possessing firearms.

6. Affiant reviewed recorded jail telephone calls made by Wilson following his arrest. Notably, on July 31, 2021, Wilson dialed telephone number 920-791-7727 and spoke with a female believed to be Angela Jones (DOB: 1993). During the call, A. Jones explained she was concerned about the firearm recovered from Wilson's vehicle during his arrest. Wilson discussed an unknown person taking ownership of the firearm and

stating they (unknown person) put the firearm in Wilson's car without Wilson's permission. Or that the unknown person could tell the police they (unknown person) forgot to remove the firearm from Wilson's car. A. Jones agreed with Wilson's comments and agreed the unknown person, referred to as "she" by A. Jones, should make those statements to law enforcement. A. Jones stated she (A. Jones) would make certain that "she" (unknown female) would make those ownership statements.

7. Affiant reviewed ATF eTrace information for the above referenced Sarsilmaz pistol bearing serial number T1102-21BV87638. Affiant learned this firearm was purchased on July 29, 2021 at Tom's Military Arms & Guns (FFL: 3-39-08841) located at 355 N. Main Street in Fond Du Lac, Wisconsin. The firearm was purchased by Brianna E. Leichtenberg (DOB: 1995). During this purchase, Leichtenberg was required to complete various documents including ATF Form 4473 which is a firearm purchase record required by federal law to be completed when a Federal Firearm Licensee (FFL) transfers a firearm to anyone who does not possess an FFL. ATF Form 4473 documents specifically which firearm/s were sold and to whom they were transferred. Leichtenberg answered "yes" to question 21(a) which stated:

> "Are you the actual transferee/buyer of the firearm(s) listed on this form? Warning: You are not the actual transferee/buyer if you are acquiring the firearm(s) on behalf of another person. If you are not the actual transferee/buyer, the licensee cannot transfer the firearm(s) to you."

8. Affiant knows, from his training and experience that individuals who cannot legally purchase firearms as a result of previous felony conviction/s will often recruit "straw purchasers" to illegally obtain firearm/s on their behalf. These "straw

purchases" are often completed with the intent to conceal the true identity of the intended recipient of the firearm. These types of transactions are commonly conducted for financial gain of the "straw purchaser" or as the result of a relationship (familial/romantic/platonic) between the previously convicted felon and the original purchaser. When a firearm is recovered by law enforcement, the firearm information is generally submitted for tracing information. This tracing information can help to identify the origin of the firearm. A common indicator of firearm straw purchasing can be relative short timespans between the purchase of a firearm and its ultimate recovery by law enforcement. Affiant is aware that illegal firearms possessors also sometimes attempt to remove the identifying information from the firearm in an attempt to conceal the origins of the firearm. Under these circumstances, the short "time to crime" and the obliterated serial number were viewed as an investigative lead into the firearm purchasing habits of Leichtenberg.

9. Affiant is aware through review of firearm purchase paperwork that the Sarsilmaz pistol bearing serial number T1102-21BV87638 was documented as being transferred to Leichtenberg at 1901 hours on July 29, 2021. Affiant is also aware the traffic stop resulting in the recovery of the aforementioned firearm and arrest of Wilson was initiated at approximately 2149 hours on July 29, 2021.

10. Affiant is aware the cellular phone recovered from Jaquan Wilson during his arrest was a black Apple iPhone with Kobe Bryant case. That cellphone was confiscated by law enforcement.

11. Affiant reviewed identifiers, such as email, telephone number, and IMEI, associated with the black Apple cellphone with the Kobe Bryant case. Using those

identifiers, Affiant reviewed data from Apple that showed Jaquan Wilson has an Apple iCloud account with username jaquanwilson674@gmail.com.

12. Affiant is aware that those who possess Apple devices often utilize Apple's iCloud services to back up and store their data in the event they need to recover information. Further, affiant is aware that this stored data can include, but is not limited to, text messages, call records, location data, photographs and videos.

13. Affiant knows that subjects involved in crimes with other subjects often need to use the cellphones to coordinate the crime. Affiant knows that subjects who trafficked firearms and illegally possess firearms often use their cellphones to take pictures of the firearms and also to take pictures of themselves with the firearms. Affiant is aware those who are prohibited from legally purchasing/possessing firearms must obtain firearms through other means, often times through a straw purchaser. A straw purchase can be described as the event where someone who can legally purchase/possess a firearm purchases a firearm on behalf of someone else. This is done in an effort to conceal the true identity of the intended recipient. Affiant is aware this is a commonly utilized technique by those previously convicted of felonies who seek to obtain firearms.

14. Affiant believes the correspondence located within the Target iCloud account will additionally provide further evidence of violations Title 18 U.S.C § 922 (g)(1), Felon in Possession of a Firearm and violations of 18 U.S.C. § 922(a)(6), commonly referred to as "lying and buying."

BACKGROUND CONCERNING APPLE

15. In my training and experience I have learned, Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

16. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to

store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

17. Apple services are accessed through the use of an "Apple ID," an account

created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

18. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

19. Additional information is captured by Apple in connection with the use of

an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

20. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

21. Apple provides users with five gigabytes of free electronic space on

iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

22. Your affiant is aware that Jaquan Wilson's iCloud account is likely to contain electronic information such as messages, call records, location data, photographs and videos. The account jaquanwilson674@gmail.com and the evidence therein would accordingly be extremely useful to the investigation. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent

from further suspicion.

23. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

24. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

25. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt

(*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

26. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

27. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

28. There is probable cause to believe that in the Apple iCloud account for Jaquan Wilson listed as jaquanwilson674@gmail.com as listed in the aforementioned paragraphs there is evidence of violations of 18 U.S.C § 922 (g)(1) Felon in Possession of a Firearm.

29. That based upon Affiant's training and experience, Affiant knows that the execution of a search warrant related to remotely stored accounts such as Apple and within email accounts maintained by Apple such as "iCloud" usually results in items of

personal documents such as bills, bank statements, photographs, videos, and other items or documents which establish the identities of persons in control of the media.

30. That based upon Affiant's training and experience, Affiant knows that individuals purchasing and selling firearms routinely keep emails, regarding the purchases and/or sales.

31. That Affiant knows that it is common for firearms purchasers and possessors to maintain electronic records, receipts, notes, ledgers, receipts relating to the transportation, ordering and purchase of firearms and that such records are typically kept where the purchaser would have ready access to them including Apple accounts.

32. That Affiant knows that firearm possessors and traffickers often take or cause to be taken photographs and other visual depictions of themselves, their associates, their property and their firearms, and typically keep and maintain these photographs in their residences and other locations where they exercise dominion and control such as telephones, tablets, computers, other media storage devices and remote storage locations.

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with jaquanwilson674@gmail.com that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B
Particular Things to be Seized

1. Information to be disclosed by Apple (Provider)

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserve, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A from 01/01/2021 to the present:

- All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses,

Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

- The contents of all emails associated with the account from 01/01/21 to present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;
- The contents of all instant messages associated with the account 01/01/21 to present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

- The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;
- All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;
- All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;
- All records pertaining to the types of service used;

- All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and
- All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

2. **Information to be seized by the government**

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C § 922 (g)(1) Felon in Possession of a Firearm and violations of 18 U.S.C. § 922(a)(6), commonly referred to as "lying and buying," those violations involving Jaquan Wilson and occurring after 01/01/21, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Records containing the sale/purchase order of ammunition in a illegal format that is intended for the military/law enforcement that would not be for public use. Records can be contained in emails, text messages, SMS messages, iMessages, etc.

(b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(e) The identity of the person(s) who communicated with the user ID about matters relating to the conspiracy and illegal importation of ammunition, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple Inc. ("Apple"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of _____ (pages/CDs/megabytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple as a regular practice; and

b. such records were generated by Apple's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Apple, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Signature